CORSO DI ALTA FORMAZIONE IN
INFORMATION SECURITY MANAGEMENT

8ª EDIZIONE, ROMA
FEBBRAIO 2011- SETTEMBRE 2011

Abuso di Internet e posta elettronica in azienda

Domande aperte e storie di vita

Michele Crudele
www.crudele.it

2011-03-25

CONSEL
CONSORZIO ELIS
per la formazione professionale superiore

CEFRIEL
FORGING INNOVATION
POLITECNICO DI MILANO

MIP
POLITECNICO DI MILANO
SCHOOL OF MANAGEMENT

ACCESSO A INTERNET IN AZIENDA

- Art. 3 della Costituzione Italiana
  - *È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese.*
  - È sufficiente per dichiarare Internet un diritto universale?
- Si può impedire l'accesso a Internet a un dipendente?
- Questioni tecniche
  - Proxy e/o firewall con pubblicazione esterna di un solo indirizzo IP
    - L'azione di uno è l'azione di tutti
  - Accesso condizionato ad autenticazione personale
    - Unicità dell'accesso e problemi connessi
  - Gli accessi autogestiti via radio e la connessione alla rete aziendale
    - Scorciatoie e rottura della protezione
    - La gestione dei portatili aziendali

POSTA ELETTRONICA IN AZIENDA

- La difesa da virus e spam
  - Necessaria analisi automatica del contenuto
  - La gestione degli aggiornamenti sui computer fissi e portatili
- L'uso personale dell'e-mail aziendale
  - Tollerato o permesso?
- Indirizzi collettivi
  - Condivisi oppure rilanciati a più utenti?
- L'accesso alla propria casella personale non aziendale
  - Situazioni particolari con protocolli e porte speciali
- I destinatari
  - Può un dipendente qualsiasi scrivere all'amministratore delegato?
  - Buone pratiche
    - Evitare messaggi destinati a tutti
    - Non mandare una critica a superiore, mettendo in copia un collega
    - Non usare la copia nascosta

DUE STORIE ITALIANE

- La conseguenza di un attacco informatico
  - Rogatoria internazionale per un attacco a sito australiano da parte di una scuola superiore di Roma
  - Situazione caotica della gestione dell'accesso a Internet per gli studenti
  - Cancellazione deliberata di tutto il server per evitare problemi di analisi dei log, prima dell'arrivo dell'autorità giudiziaria
- La conseguenza di un insulto
  - Una persona scrive in forma anonima un insulto su una pagina della Wikipedia
  - Tutta la rete aziendale, che esce con lo stesso IP, viene bandita da Wikipedia e nessuno può più fare modifiche in forma anonima
  - Resta il marchio di "infamia" nelle pagine di Wikipedia

FILTERING

- URL filtering
  - Elenco di siti da bloccare: black list
    - Non efficace su domini con sottodomini e sui social networks
  - Elenco di siti permessi: white list
    - Biblioteca di casa, walled garden
    - Limitativo ma molto sicuro
- Content filtering
  - Analisi istantanea del contenuto della pagina web
    - Confronto con elenco di categorie permesse
    - Fortemente dipendente dalla lingua
    - Ambiguità e falsi positivi e negativi

www.ilFiltro.it per maggiori dettagli e test di sistemi ad uso familiare

DISCIPLINARE RISORSE INFORMATICHE

- Richiesto dalle Linee guida del Garante per posta elettronica e internet
  - Contengono principi, prescrizioni e divieti
  - Punto di riferimento per il tema
- Contenuti dipendenti dalla complessità dell'azienda
- Accordo sindacale oppure firma dell'utente per accettazione
- Aggiornamento periodico
- Legame con il DPS – documento programmatico sulla sicurezza

GLI OSPITI IN AZIENDA

- Decreto Pisanu: non più valido
  - Imponeva il riconoscimento di tutti coloro che accedevano a Internet tramite un fornitore di connettività
  - Promulgato per identificare i terroristi in rete
  - Era accettata di fatto la procedura di riconoscimento via SMS
    - Usata da Provincia di Roma
    - Era un vero ostacolo alla diffusione del WiFi libero?
- Scenari diversi
  - Una utenza *guest* uguale per tutti
    - Nessun lavoro di gestione, molti guai potenziali
  - Una *scratch card* a ogni utente con limite temporale
    - Poco lavoro di gestione, difficoltà di identificare gli autori di illeciti
  - Un *account* temporaneo
    - Molto lavoro di gestione, facilità di identificare gli autori di illeciti

TO LOG OR NOT TO LOG

- *Traffic Reports*
- *Protocol Usage Reports*
- *Web Usage Reports*
- *Mail Usage Reports*
- *FTP Usage Reports*
- *Telnet Usage Reports*
- *Event Summary Reports*
- *VPN Usage Reports*
- *Firewall Rules Report*
- *Inbound Outbound Reports*
- *Intranet Reports*
- *Internet Reports*
- *Streaming & Chat Sites Reports*
- *Security Reports*
- *Virus Reports*
- *Attack Reports*
- *Admin Reports*

Statistiche aggregate o analisi puntuale?

UNA STORIA VERA: DI CHI È LA COLPA?

- Un documento del “grande capo” va in giro per tutta l’azienda
- Il capo si “arrabbia” perché non l’ha diffuso lui
- Chiede a un consulente esterno un’indagine sulla sicurezza
- Il consulente verifica che l’azienda ha un ottimo sistema ma…
  - consiglia al capo di cambiare il suo computer con Windows 95 perché poco protetto
- I responsabili della sicurezza informatica glielo avevano già detto da tempo, ma lui non aveva voluto cambiare
  - Tutto il suo disco era accessibile a chiunque dalla rete aziendale

CHE COSA FARE IN QUESTI CASI?

WEB 2.0 E L'AZIENDA

- Uso di social networks in azienda per fini personali
  - Perdita di tempo
  - Commenti negativi sull'azienda
  - Proibirli tutti?
- Social networks aziendali
  - Interni
    - Scambio di idee, ma anche di critiche
  - Esterni
    - Se monitorati possono essere utili al marketing
    - Richiedono molto tempo degli esperti di comunicazione

SENZA FILI

- Protezione della WLAN aziendale
  - Aperta per accesso a Internet con web authentication e senza accesso a dati aziendali
  - Protetta WPA2 con autenticazione personale per accesso a dati aziendali
    - Richiede la diffusione della chiave
  - 802.1x (EAP) con server RADIUS
    - TLS richiede installazione di certificati sui dispositivi
- Problemi di accessibilità in presenza di molti access point diversi contemporanei
- Facilità di intercettazione di dati dei social networks su reti wireless